



National Aeronautics and
Space Administration

John C. Stennis Space Center
Stennis Space Center, MS
39529-6000

SPR 2810.1 Basic
October 2004

COMPLIANCE IS MANDATORY

John C. Stennis Space Center Public Key Infrastructure (PKI) Procedural Requirements

Stennis Procedural Requirements	SPR 2810.1	Basic
	Number	Rev.
	Effective Date: October 27, 2004	
	Expiration Date: August 3, 2009	
	Page i of viii	
Responsible Office: Center Operations Directorate		
SUBJECT: SSC Public Key Infrastructure (PKI) Procedural Requirements		

Document History Log

Status/Change/ Revision	Change Date	Originator/Phone	Description
SPG 2810.1 Basic	10/30/99	SSC PKI Team POC Renay Nelson (228) 688-1585	SPG 2810.1 Basic, Initial Release
SPG 2810.1 A	06/3/03	Renay Nelson x 8-1585	General revision to correct format, provide clarity, and reflect changes in organization names, responsibilities, and process.
SPR 2810.1 Basic *Note: The original history of the prior Directive has been retained here to provide clarity and for tracking and reference purpose.	10/25/2004	Renay Nelson	Initial issuance as a new Directive. Revalidated per NASA rules review. New corrected number assigned and changed to SPR.

Stennis Procedural Requirements	SPR 2810.1	Basic
	<i>Number</i>	<i>Rev.</i>
	Effective Date: October 27, 2004	
	Expiration Date: August 3, 2009	
	Page ii of viii	
Responsible Office: Center Operations Directorate		
SUBJECT: SSC Public Key Infrastructure (PKI) Procedural Requirements		

Table of Contents

PREFACE	v
P.1 PURPOSE.....	v
P.2 APPLICABILITY	v
P.3 AUTHORITY	vi
P.4 REFERENCES	vi
P.5 MEASUREMENTS	vii
P.6 CANCELLATION	viii
CHAPTER 1. INTRODUCTION	1
1.1 PKI Overview	1
1.2 Application of PKI	1
1.3 Limitations to Reliance on PKI	2
1.4 Purpose and Scope	2
1.5 Required References.....	2
1.6 Acronyms and Definitions.....	3
CHAPTER 2. ROLES AND RESPONSIBILITIES	4
2.1 NASA Organizational Hierarchy	4
2.2 SSC Organization and Management Responsibility	4
2.2.1 Organization.....	4
2.2.2 SSC Center Director	6
2.2.3 Center Operations Directorate	6
2.2.4 Center IT Security Manager / PKI Operational Authority and Registration Authority Administrator	6
2.2.5 SSC Chief of Security	7
2.2.6 SSC Security Services Contractor/RA Authenticator.....	7
2.2.7 SSC Information Technology Services Contractor/PKI Registration Authority (RA).....	8
2.2.8 ITS IT Security Liaison and IPSO Information Technology Security Officer	9
2.2.9 SSC ODIN Contractor	9
2.2.10 NASA/NASA Contractor Human Resource Offices	9
2.2.11 Organization Managers	10
2.2.12 Employees.....	10
CHAPTER 3. PROCESSES AND PROCEDURES	11
3.1 PKI Processes	11
3.2 Application for PKI Certificate	11
3.2.1 When to Use Application Process	11
3.2.2 Who May Apply	11
3.2.3 Eligibility and System Requirements	12

Stennis Procedural Requirements	SPR 2810.1	Basic
	<i>Number</i>	<i>Rev.</i>
	Effective Date: October 27, 2004	
	Expiration Date: August 3, 2009	
	Page iii of viii	
Responsible Office: Center Operations Directorate		
SUBJECT: SSC Public Key Infrastructure (PKI) Procedural Requirements		

3.2.4	Certificate Application Procedure	15
3.3	PKI Certificate Revocation and Suspension/Disabling Process.....	16
3.3.1	When to Use Revocation and Suspension/Disabling Process	17
3.3.1.1	Revocation	17
3.3.1.2	Suspension/Disabling.....	18
3.3.1.3	Accidental Key Compromise.....	18
3.3.2	Who May Request.....	18
3.3.3	Reinstatement of Revoked Privileges	18
3.3.4	Revocation and Suspension/Disabling Procedure	20
3.4	Key Recovery Process.....	21
3.4.1	Who May Request.....	21
3.4.2	When to Use the Key Recovery Process.....	22
3.4.2.1	User Requests for Key Recovery	23
3.4.2.2	Non-User-Consent Key Recovery	23
3.4.2.3	Should Key Recovery Be Performed?	24
3.4.3	Key Recovery Procedure	24
3.5	Help Desk – Ext. 2525.....	25
3.6	RA Facility Security and Access.....	26
3.7	Software Distribution and Control	27
3.7.1	Entrust Software Training and Installation.....	28
3.7.2	Software Removal and Account Terminations	28
3.7.3	Entrust Software Maintenance.....	28
3.8	Documentation and Data Control.....	28
	APPENDICES	30
	Appendix A: Acronyms	31
	Appendix B: Definitions	32
	ATTACHMENTS.....	34
	Attachment A: SSC PKI Key Personnel and Critical Contacts	35
	Attachment B: Nondisclosure Agreement	36
	Attachment C: PKI Certificate Issuance and Account Information Memorandum.....	37
	Attachment D: Acknowledgement of Receipt of Authorization and Account Information	39
	Attachment E: Notification of Revocation or Disabling/Suspension Action	40
	Attachment F: Acknowledgement of Receipt of Revocation or Suspension/Disabling Notification	41

Stennis Procedural Requirements	SPR 2810.1	Basic
	<i>Number</i>	<i>Rev.</i>
	Effective Date: October 27, 2004	
	Expiration Date: August 3, 2009	
	Page iv of viii	
Responsible Office: Center Operations Directorate		
SUBJECT: SSC Public Key Infrastructure (PKI) Procedural Requirements		

Figures

Figure 2.1 – NASA PKI Organizational Hierarchy	4
Figure 2.2 – SSC PKI Registration Authority (RA) Functional Organization	5
Figure 3.1 – Basic PKI Processes	13
Figure 3.2 – Certificate Application and Approval Process	14
Figure 3.3 – Revocation and Suspension/Disabling Process	19
Figure 3.4 – Key Recovery Process	22

Tables

Table 1 System Requirements for PKI	12
---	----

Stennis Procedural Requirements	SPR 2810.1	Basic
	<i>Number</i>	<i>Rev.</i>
	Effective Date:	October 27, 2004
	Expiration Date:	August 3, 2009
Page v of viii		
Responsible Office: Center Operations Directorate		
SUBJECT: SSC Public Key Infrastructure (PKI) Procedural Requirements		

PREFACE

P.1 PURPOSE

The National Aeronautics and Space Administration (NASA) has implemented Public Key Infrastructure (PKI) to provide security for its electronic information. This PKI consists of systems, products, and services, which provide and manage X.509 certificates for public-key cryptography.

The Policy Authority (PA), responsible for setting, implementing, and administering policy for the NASA PKI, is vested in the NASA Chief Information Officer. The NASA CIO has appointed Ames Research Center (ARC), in collaboration with the Enterprise Associate Administrators and Institutional Program Offices, as the Principal Center for Information Technology (IT) Security. In this role, ARC is responsible for establishing and maintaining the policies, practices, and procedures implementing and governing the PKI program as well as the necessary PKI infrastructure to support the Certification Authority (CA). Each NASA Center is responsible for establishing and operating a center-wide Registration Authority (RA) operating under the cognizance of the CA.

The “X.509 Certificate Policy for National Aeronautics and Space Administration (NASA) Public Key Infrastructure (PKI)” and other documents issued by ARC define the NASA PKI policy and how the PKI will be established and operated. This policy governs Certification Authorities (CA’s) within the NASA PKI and by CA’s outside the NASA PKI who wish to inter-operate with CA’s within the NASA PKI.

The purpose of this “SSC Procedural Requirements for Public Key Infrastructure” is to implement requirements of the NASA PKI program in compliance with the “X.509 Certificate Policy.” This SPR establishes the responsibilities, procedures, and requirements for implementing the SSC RA, and for operating, and using the PKI at the John C. Stennis Space Center.

P.2 APPLICABILITY

NASA policy for PKI applies to the confidentiality and integrity of data exchange through encryption and for digitally signed documents among NASA employees, grantees, and contractors acting on NASA’s behalf, regardless of location.

A public key Certificate:

- Is not to be applied for protection of classified information; and
- Does not imply that the Subscriber has any authority to conduct business transactions on behalf of the organization operating the NASA Certificate Authority.

Stennis Procedural Requirements	SPR 2810.1	Basic
	<i>Number</i>	<i>Rev.</i>
	Effective Date:	October 27, 2004
	Expiration Date:	August 3, 2009
Responsible Office: Center Operations Directorate		
SUBJECT: SSC Public Key Infrastructure (PKI) Procedural Requirements		
Page vi of viii		

This SPR specifically applies to all NASA and NASA Contractor employees of the John C. Stennis Space Center for the establishment, operation, maintenance, and use of the PKI.

P.3 AUTHORITY

- a. 40 U.S.C. 759 note, the Computer Security Act, P.L. 100-235, as amended.
- b. 42 U.S.C. 2451, et. seq., the National Aeronautics and Space Act of 1958, as amended.
- c. 18 U.S.C. 799, et. seq., Violation of regulations of National Aeronautics and Space Administration.
- d. 5 U.S.C. 552, et. seq., the Freedom of Information Act, as implemented by 14 CFR 1201.
- e. 5 U.S.C. 552a, the Privacy Act, P.L. 93-579, as amended.
- f. 40 U.S.C. 1401, et. seq., Section 808 of Public Law 104-208, the Clinger-Cohen Act of 1996 [renaming, in pertinent part, the Information Technology Management Reform Act (ITMRA), Division E of Public Law 104-106].
- g. 50 U.S.C. 2401-2420, the Export Administration Act of 1979, as amended, as implemented by the Export Administration Regulations, 15 CFR Part 730-774.
- h. 18 U.S.C. 2510, et. seq., the Electronic Communications Privacy Act, as amended.
- i. 44 U.S.C. 2510, et. seq., the Paperwork Reduction Act of 1995, P.L. 104-13, as amended.
- j. Executive Order No. 12958, Classified National Security Information of May 18, 1995.
- k. Executive Order No. 13011, Federal Information Technology of July 16, 1996.

OMB Circular No. A-130, Management of Federal Information Resources.

P.4 REFERENCES

- a. NPR 2800.1, Managing Information Technology.
- b. NPR 2800.1, Managing Information Technology.
- c. NPR 2810.1, Security of Information Technology.
- d. NPR 2810.1, Security of Information Technology.
- e. NPR 2820.1, NASA Software Policies.
- f. NPR 1600.2, NASA Security Policy.

Stennis Procedural Requirements	SPR 2810.1	Basic
	<i>Number</i>	<i>Rev.</i>
	Effective Date:	October 27, 2004
	Expiration Date:	August 3, 2009
Page vii of viii		
Responsible Office: Center Operations Directorate		
SUBJECT: SSC Public Key Infrastructure (PKI) Procedural Requirements		

- g. NPR 1620.1, Security Procedures and Guidelines.
- h. NPR 1382.17, Privacy Act – Internal NASA Direction in Furtherance of NASA Regulations.
- i. NPR 9800.1, NASA Office of Inspector General Programs.
- j. NPR 1441.1, NASA Electronic Mail.
- k. SPR 2800.1, SSC Information Technology Resources Usage Policy.
- l. SPR 1620.6, Protection of Personal Privacy – (SSC) Privacy Act Regulations.
- m. X.509 Certificate Policy for National Aeronautics and Space Administration (NASA) Public Key Infrastructure; Information Technology Security Development Group, Applied Information Technology Division, Code JT, NASA Ames Research Center.
- n. NASA Certification Authority Certification Practice Statement (CPS); Information Technology Security Development Group, Applied Information Technology Division, Code JT, NASA Ames Research Center.
- o. NASA Public Key Infrastructure Practices; Information Technology Security Development Group, Applied Information Technology Division, Code JT, NASA Ames Research Center.
- p. NASA PKI Registration Authority (RA) Operations Manual; Information Technology Security Development Group, Applied Information Technology Division, Code JT, NASA Ames Research Center.
- q. Registration Authority (RA) Test Scripts for the Entrust/RA Software; Information Technology Security Development Group, Applied Information Technology Division, Code JT, NASA Ames Research Center.

P.5 MEASUREMENTS

The effectiveness of this SPR will be evaluated using external and internal audits performed by a mix of CA, NASA, and contractor personnel. Management reviews are conducted to ensure the suitability and effectiveness of the documents and processes that implement the PKI.

Stennis Procedural Requirements	SPR 2810.1		Basic
	Number	Rev.	
	Effective Date: October 27, 2004		
	Expiration Date: August 3, 2009		
	Page viii of viii		
Responsible Office: Center Operations Directorate			
SUBJECT: SSC Public Key Infrastructure (PKI) Procedural Requirements			

P.6 CANCELLATION

SPR 2810.1 Basic

Signature on file

T. Q. Donaldson V, RDML USN (Ret)
Director

DISTRIBUTION

Approved for public release via NODIS; distribution is unlimited

Stennis Procedural Requirements	SPR 2810.1	Basic
	Number	Rev.
	Effective Date: October 27, 2004	
	Expiration Date: August 3, 2009	
Responsible Office: Center Operations Directorate		Page 1 of 41
SUBJECT: SSC Public Key Infrastructure (PKI) Procedural Requirements		

CHAPTER 1. INTRODUCTION

1.1 PKI Overview

The National Aeronautics and Space Administration (NASA) Public Key Infrastructure (PKI) is an agency-wide system for providing security for transmittal of electronic information. The PKI uses certificates for electronic information confidentiality and integrity through the use of encryption and digital signatures, respectively. A PKI provides desktop security, as well as security for desktop and network applications, including electronic and Internet commerce.

The PKI system manages digital encryption keys used to lock and unlock computer data. The basic purpose of a PKI is to enable an End User to share personal data keys with other Users in a secure manner. Keys come in pairs of one encryption key pair and one signing key pair. Encrypted data may be retrieved and read only by individuals possessing a corresponding key to unlock the data file. For security of the signature process, the PKI system does not manage private signing keys to which only Users have access. Keys are authorized and managed by means of Certificates. The X.500 Directory System is the management tool and repository for certificates. Specifically, the PKI:

- Allows End Users to send and receive secure packages (files) to and from anyone in the Agency who also has PKI;
- Allows an End User to digitally sign reports and documents and ensures that the signature or document is not altered in any way en route to a recipient;
- Verifies the digital signature of the person who signed the file to ensure that the file actually came from that person;
- Guarantees that only the person whose digital signature appears is the signatory of a particular document or the executor of a particular transaction;
- Assures that file contents remain unchanged from the time the document is signed; and
- Provides and assures that only the owner of the particular private signing key can use the personal signature of the owner.

1.2 Application of PKI

The use of the NASA PKI is suitable for the protection of NASA-sensitive unclassified data such as:

- Contractor information provided to NASA that is subject to the terms of NASA's standard non-disclosure agreement;
- Contract and proposal planning, design, development, and testing documentation;
- Project and budget planning, tracking, and reporting;

Stennis Procedural Requirements	SPR 2810.1	Basic
	<i>Number</i>	<i>Rev.</i>
	Effective Date: October 27, 2004	
	Expiration Date: August 3, 2009	
Responsible Office: Center Operations Directorate		
SUBJECT: SSC Public Key Infrastructure (PKI) Procedural Requirements		

- Personnel information, including position, salary, benefits, and medical records; and
- Electronic commerce transactions including EDI, e-mail, Web servers, SSL, etc.

Other applications may be included or excluded as they are identified.

1.3 Limitations to Reliance on PKI

In the NASA PKI Certification Authority (CA) domain, all Users are both requesters and relying parties. Users, as relying parties, shall limit reliance on PKI as follows:

- Restrict reliance on NASA issued certificates to appropriate uses for those certificates in accordance with the policy under which the certificate was issued and the NASA PKI Practices;
- Verify certificates including revocation lists in consideration of critical extensions; and
- Trust and make use of certificates only if a valid certificate chain is established between the relying party and the certificate subject.

1.4 Purpose and Scope

This requirement:

- Identifies and implements SSC requirements for establishing and operating the PKI in compliance with the “X.509 Certificate Policy (CP) for NASA Public Key Infrastructure” and the practices established by the NASA Certificate Authority (CA) in the “NASA Certification Authority Certification Practice Statement” and the “NASA Public Key Infrastructure Practices”;
- Identifies the structure, roles, relationships, and responsibilities for implementing, managing, operating, and using the PKI at SSC; and
- Provides the processes and procedures for administering the SSC PKI and issuing, using, and revoking PKI encryption certificates.

The roles, relationships, and responsibilities for implementing, managing, operating, and using the PKI at SSC are defined in Chapter 2 of this document. Chapter 3 provides the processes and procedures that all SSC PKI Users must follow. Supplemental information is provided in the appendixes and attachments to this document.

1.5 Required References

A list of references is provided in the Preface to this document. The NASA Policy Authority is responsible for maintaining the PKI program policy documentation and procedures. Users will be required to acknowledge they have read and understand PKI requirements upon application and prior to issuance of their personal PKI certificate. SSC PKI Users should refer to these

Stennis Procedural Requirements	SPR 2810.1	Basic
	<i>Number</i>	<i>Rev.</i>
	Effective Date: October 27, 2004	
	Expiration Date: August 3, 2009	
		Page 3 of 41
Responsible Office: Center Operations Directorate		
SUBJECT: SSC Public Key Infrastructure (PKI) Procedural Requirements		

documents for information and instructions as needed. The key required reference documents and other instructional information are provided on-line at: <http://nasaca.nasa.gov/docs.html> and <http://pki.nasa.gov/newuser.html>.

1.6 Acronyms and Definitions

Acronyms and definitions are provided in Appendixes A and B.

Stennis Procedural Requirements	SPR 2810.1	Basic
	<i>Number</i>	<i>Rev.</i>
	Effective Date: October 27, 2004	
	Expiration Date: August 3, 2009	
Responsible Office: Center Operations Directorate		Page 4 of 41
SUBJECT: SSC Public Key Infrastructure (PKI) Procedural Requirements		

CHAPTER 2. ROLES AND RESPONSIBILITIES

2.1 NASA Organizational Hierarchy

The NASA PKI organizational hierarchy is depicted in Figure 2.1. Responsibility for NASA PKI administrative and operational functions is centralized under the NASA Certification Authority at the Ames Research Center (ARC). NASA Centers operate as Registration Authorities under the cognizance of the CA. SSC functional and organizational responsibilities are defined in the following paragraphs. A listing of SSC key contact personnel performing the various SSC RA functions is provided in Attachment A. This listing, which also includes other critical contacts, is maintained by the SSC RA and is updated on a periodic basis.

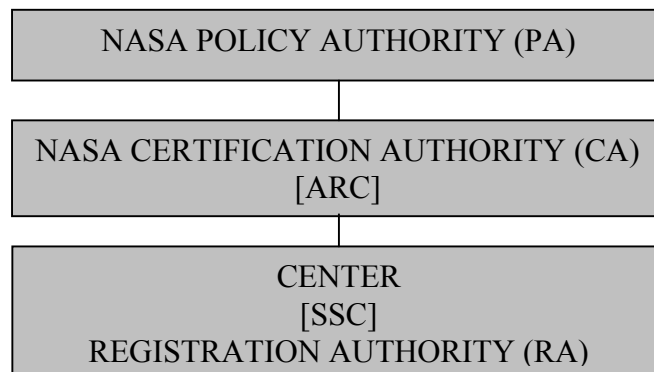


Figure 2.1 – NASA PKI Organizational Hierarchy

2.2 SSC Organization and Management Responsibility

Responsibility for administration, management, and execution of SSC PKI System Registration Authority functions is distributed across Center organizations.

2.2.1 Organization

The SSC PKI functional organization chart, showing the lines of authority from the Center Director to End Users, is shown in Figure 2.2.

Stennis Procedural Requirements	SPR 2810.1	Basic
	<i>Number</i>	<i>Rev.</i>
	Effective Date: October 27, 2004	
	Expiration Date: August 3, 2009	
Responsible Office: Center Operations Directorate		
SUBJECT: SSC Public Key Infrastructure (PKI) Procedural Requirements		
Page 6 of 41		

2.2.2 SSC Center Director

The total operational control of SSC rests with the Center Director. For PKI, the Director is responsible for:

- a. Ensuring the establishment and operation of the center-wide PKI system and Registration Authority;
- b. Appointing in writing Registration Authority Administration personnel;
- c. Ensuring the most effective and efficient implementation of the PKI policies and procedures; and
- d. Providing sufficient resources (including trained personnel) for management, performance of work, verification, and auditing functions.

2.2.3 Center Operations Directorate

Responsibility for PKI RA administration and management is delegated to the SSC Center Operations, Office of Chief Information Officer. Responsibility within the Office of Chief Information Officer for the administrative oversight and operations of the RA function is delegated to the SSC Information Technology (IT) Security Manager and designated IT personnel of the Office of Chief Information Officer. The IT Security Manager and the Office of Chief Information Officer are the responsible authorizing entities for SSC PKI activities including but not limited to:

- a. Assurance of User training on PKI software use;
- b. PKI software;
- c. Operation of the Registration Authority; and
- d. Issuance and revocation of PKI Certificates and PKI key recovery.

2.2.4 Center IT Security Manager / PKI Operational Authority and Registration Authority Administrator

The SSC IT Security Manager (C-ITSM) is the local PKI Operational Authority and is responsible for the overall RA function. The IT Security Manager reports to the Office of Chief Information Officer Director within the Center Operations Directorate. The C-ITSM is responsible for:

Registration Authority Administration;

- a. Validating end entity requests and requirements for PKI actions;

Stennis Procedural Requirements	SPR 2810.1	Basic
	<i>Number</i>	<i>Rev.</i>
	Effective Date: October 27, 2004	
	Expiration Date: August 3, 2009	
Responsible Office: Center Operations Directorate		Page 7 of 41
SUBJECT: SSC Public Key Infrastructure (PKI) Procedural Requirements		

- b. Initiating/authorizing key applications, suspensions, revocations, or recoveries in accordance with PKI policy;
- c. Dispute Resolution;
- d. Operational monitoring and performance of audits to ensure compliance with NASA and SSC PKI policies and practices;
- e. Development of IT incident reporting, response and investigation plans and procedures;
- f. Initiating, coordinating, investigating, and resolving IT security incidents;
- g. Maintaining records of IT security incidents and logbooks of PKI actions; and
- h. Maintaining a secure environment for PKI actions and information.

The C-ITSM, along with the Office of Chief Information Officer, monitors the Information Technology Services Contractor's day-to-day management of the Stennis Data Center (SDC) [formerly Program Support Computer Systems - PSCS] and its operations to implement, support, and maintain the PKI system and its RA functions at SSC.

2.2.5 SSC Chief of Security

The SSC Chief of Security (CCS) is responsible for ensuring overall SSC physical security. The Chief of Security:

- a. Coordinates and monitors the activities of the SSC Security Services Contractor;
- b. Conducts and/or assists in security incident investigations; and
- c. Coordinates and processes personnel background investigations as needed for security clearances and positions of trust in conjunction with the Human Resources Office.

The SSC Chief of Security reports to the Center Services Division Chief within the Center Operations Directorate.

2.2.6 SSC Security Services Contractor/RA Authenticator

The SSC Security Services Contractor is responsible for maintenance for the SSC Badging Systems, validation of identity for and issuance of personnel badges, verification of badge numbers, and performance of necessary security checks for RA requirements. The Security Services Contractor provides physical security for the SSC facility under the cognizance of the SSC Chief of Security.

Stennis Procedural Requirements	SPR 2810.1	Basic
	<i>Number</i>	<i>Rev.</i>
	Effective Date: October 27, 2004	
	Expiration Date: August 3, 2009	
Page 8 of 41		
Responsible Office: Center Operations Directorate		
SUBJECT: SSC Public Key Infrastructure (PKI) Procedural Requirements		

2.2.7 SSC Information Technology Services Contractor/PKI Registration Authority (RA)

The Stennis Data Center is the Center's Information Processing Service Organization (IPSO). Operated by the SSC Information Technology Services Contractor (ITS), the SDC is the implementing PKI RA organization and is responsible for day-to-day RA functions including PKI system administration. The RA utilizes the SSC Badging System maintained by the Security Services Contractor for identity and verification functions. The SDC serves as the Registration Authority under the direction of the C-ITSM. The RA is responsible for:

- a. Installation, maintenance and operation of the PKI system and performance of regular system backups;
- b. Ensuring physical security of the PKI system and the information contained therein;
- c. Establishing procedures for RA functions and maintaining records and logbooks of all PKI actions;
- d. Identifying and authenticating the identity of certificate applicants and other action requesters with the SSC Badging Systems and X.500 Directory;
- e. Withholding necessary information for initialization of actions when there is lack of proper identification by end entities or other requesters;
- f. Receiving and distributing subscriber authorization information and issuing new key pairs for Users;
- g. Performing certificate and key management functions (e.g., enabling, disabling, or suspending User certificates, updating certificates/keys, revoking certificates and managing key recovery for end entities);
- h. Changing the User Distinguished Name (DN) on certificates in cooperation with the Center's X.500 Directory Administrator;
- i. Viewing audit logs and reporting suspicious events to the IT Security Manager and CA officers;
- j. Creating various reports of User status;
- k. Acting as intermediary Help Desk resource for resolution of User problems and questions; and
- l. Holding in confidentiality all personal and proprietary information relative to PKI transactions and operations.

The ITS Operations Manager of the SDC is responsible for supervision of RA personnel and PKI operations. The ITS will ensure adequate trained resources for the performance of work requirements. A minimum of two personnel will be trained as RA's and one or more additional persons will be trained as Registration Authority System Administrator (RASA). The SDC PKI RA will provide normal weekday hours of operation to coincide with NASA/SSC PKI

Stennis Procedural Requirements	SPR 2810.1	Basic
	Number	Rev.
	Effective Date: October 27, 2004	
	Expiration Date: August 3, 2009	
Responsible Office: Center Operations Directorate		Page 9 of 41
SUBJECT: SSC Public Key Infrastructure (PKI) Procedural Requirements		

requirements. All RA personnel will be cleared for “Positions of Trust” and sign non-disclosure agreements.

2.2.8 ITS IT Security Liaison and IPSO Information Technology Security Officer

The ITS IT Security Liaison assists and supports the SSC IT Security Manager in:

- a. Facility IT security planning;
- b. Day-to-day operational IT Security issues;
- c. IT security monitoring; and
- d. Site IT incident response and resolution.

The ITS Manager of the SDC serves as the IPSO Information Technology Security Officer (ITSO) and is responsible for security of the SDC and PKI RA operations. The ITSO manages and coordinates security planning, issues, and problem resolution for the IPSO with the ITS IT Security Liaison and the NASA/SSC IT Security Manager.

2.2.9 SSC ODIN Contractor

The SSC ODIN Contractor is responsible for administering and maintaining X.500 Directory services and appropriate Entrust software load and configuration as defined by NASA contract agreement.

2.2.10 NASA/NASA Contractor Human Resource Offices

NASA and NASA Contractor Human Resource offices are responsible for:

- a. Verifying personal information (i.e., identity, social security number, date and place of birth, etc.) for all personnel at time of in-processing and request for badge issuance;
- b. Coordinating appropriate personnel security background checks with NASA, corporate or other security offices commensurate with “critical-sensitive positions” or “positions of trust”;
- c. Providing personnel training regarding conflicts of interest and non-disclosure of information in compliance with Federal regulations, NASA policy, and/or contract provisions;
- d. Obtaining employee’s signature on non-disclosure agreement regarding privacy act, critical-sensitive, or proprietary information; and
- e. Maintaining appropriate records of personal information, background investigations, and non-disclosure agreements.

An example of a typical nondisclosure agreement is provided as Attachment B. Words and structure of the agreement may vary from organization to organization.

Stennis Procedural Requirements	SPR 2810.1	Basic
	<i>Number</i>	<i>Rev.</i>
	Effective Date: October 27, 2004	
	Expiration Date: August 3, 2009	
Responsible Office: Center Operations Directorate		Page 10 of 41
SUBJECT: SSC Public Key Infrastructure (PKI) Procedural Requirements		

2.2.11 Organization Managers

Organization managers are responsible for:

- a. Validating and approving end-user requirements for PKI;
- b. Requesting or approving User or other end-entity requests for certificate application, disabling, suspension, revocation, or key recovery;
- c. Reporting key compromises, suspected compromises, or personnel dismissals for cause to the SSC IT Security Manager and PKI RA; and
- d. Prompt reporting of personnel terminations or changes in responsibility.

2.2.12 Employees

All employees are responsible for using the PKI in accordance with policy and procedures, and reporting violations or suspected violations. End Users or other requesters are responsible for:

- a. Presenting accurate and true information in certificate application, suspension/disabling, revocation, and key recovery requests;
- b. Completing End User PKI training;
- c. Obtaining PKI software and its installation only through the appropriate authorized channels;
- d. Creating a username with the authorization information provided by the RA;
- e. Using encryption and signing capabilities responsibly, and in accordance with NASA policies on use of government supplied equipment and software;
- f. Reading and understanding PKI policies and procedures and acknowledging same;
- g. Ensuring that private keys and passwords are protected;
- h. Ensuring that User files are backed up;
- i. Securing and protecting personal profiles from access by unauthorized persons;
- j. Notifying the RA upon private key compromise or suspected compromise; and
- k. Notifying the RA when a Certificate is no longer needed, upon termination or long-term absence, or upon changes in responsibility or personal User information (name, work or home addresses, phone, affiliation, etc.).

Stennis Procedural Requirements	SPR 2810.1	Basic
	<i>Number</i>	<i>Rev.</i>
	Effective Date: October 27, 2004	
	Expiration Date: August 3, 2009	
Responsible Office: Center Operations Directorate		Page 11 of 41
SUBJECT: SSC Public Key Infrastructure (PKI) Procedural Requirements		

CHAPTER 3. PROCESSES AND PROCEDURES

3.1 PKI Processes

PKI processes are encompassed in three primary areas of activity:

1. Application.
2. Revocation or Suspension/Disabling.
3. Key Recovery.

Figure 3.1 illustrates the basic processes to follow for different types of problems, questions, or requirements.

3.2 Application for PKI Certificate

All personnel must apply for an account (i.e., Certificate) in order to access and use the PKI system. The Certificate provides the authorization code to access the system and set up the User's personal profile. To obtain a Certificate, Users must complete the NASA/SSC PKI Certificate Application and Approval Request form and complete training on the use of PKI. Complete instructions are provided with the form. The form must be filled out legibly and completely. Users shall read and follow all instructions. Any form lacking information will be disregarded. A flowchart of the Certificate application and approval process is presented in Figure 3.2. SSC forms are available under "Forms" on the SSC Intranet internal home page.

3.2.1 When to Use Application Process

The application process is used to:

1. Request a new User Account for an individual or non-human entity (e.g., processor or server)
2. Change User information (name, address, phone, personal information, affiliation, organization, etc.)
3. Re-enable a disabled User Account

It is the User's responsibility to promptly report and record all changes in account information.

3.2.2 Who May Apply

Any SSC employee with a valid need for PKI may apply for a PKI Certificate. Certificates may also be issued to a non-human end entity, e.g., a processor or server. In this case, the person responsible for the system must apply for and maintain the certificate for the entity.

Stennis Procedural Requirements	SPR 2810.1	Basic
	Number	Rev.
	Effective Date: October 27, 2004	
	Expiration Date: August 3, 2009	
Responsible Office: Center Operations Directorate		Page 12 of 41
SUBJECT: SSC Public Key Infrastructure (PKI) Procedural Requirements		

Examples of suitable applications for PKI are given in Paragraph 1.2. User management and the SSC IT Security Manager will validate requirements and suitability of purpose.

3.2.3 Eligibility and System Requirements

Requesters must satisfy the following eligibility requirements:

1. You must have a NASA photo ID badge
2. You must have an SSC e-mail account and an entry in the X.500 directory
3. Your PC must satisfy the minimum hardware/software system requirements
4. You must read and understand the conditions of issuance (<http://nasaca.nasa.gov/docs.html>)
5. You must complete PKI End User training (<http://pki.nasa.gov/newuser.html>).

System Requirements are provided in the following table.

Table 1 System Requirements for PKI

*Windows PC	*Macintosh Power PC	*UNIX
486 microprocessor or better	Macintosh 68020 or higher	Solaris 2.4 & above
16 Mbytes of RAM	Power PC processor	HP-UX 10.20
50 Mbytes of free disk space on hard drive	Macintosh System 7.1 or higher	AIX 4.3
Network connection ready		
Microsoft Windows 95 (service pack 1 or higher)		
Microsoft Windows 98		
Microsoft Windows NT (service pack 5 or higher)		

*Check requirements with the Information Management Division for systems other than those shown.

Stennis Procedural Requirements	Number	SPR 2810.1	Rev.	Basic
Effective Date: October 27, 2004				
Expiration Date: August 3, 2009				
Responsible Office: Center Operations Directorate		Page 13 of 41		
SUBJECT: SSC Public Key Infrastructure (PKI) Procedural Requirements				

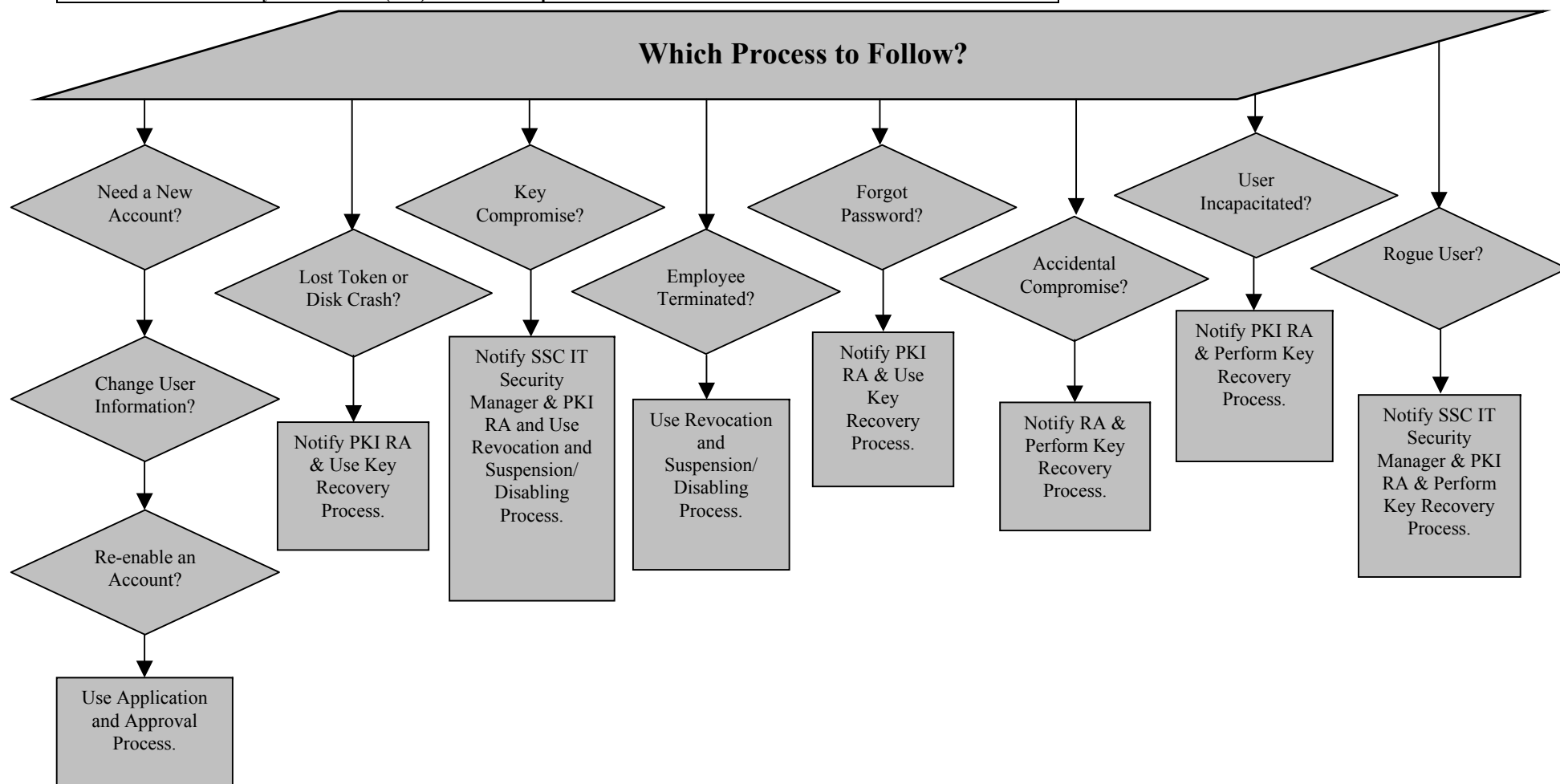


Figure 3.1 – Basic PKI Processes

Stennis Procedural Requirements	SPR 2810.1	Basic
	Number	Rev.
	Effective Date: October 27, 2004	
	Expiration Date: August 3, 2009	
Page 14 of 41		
Responsible Office: Center Operations Directorate		
SUBJECT: SSC Public Key Infrastructure (PKI) Procedural Requirements		

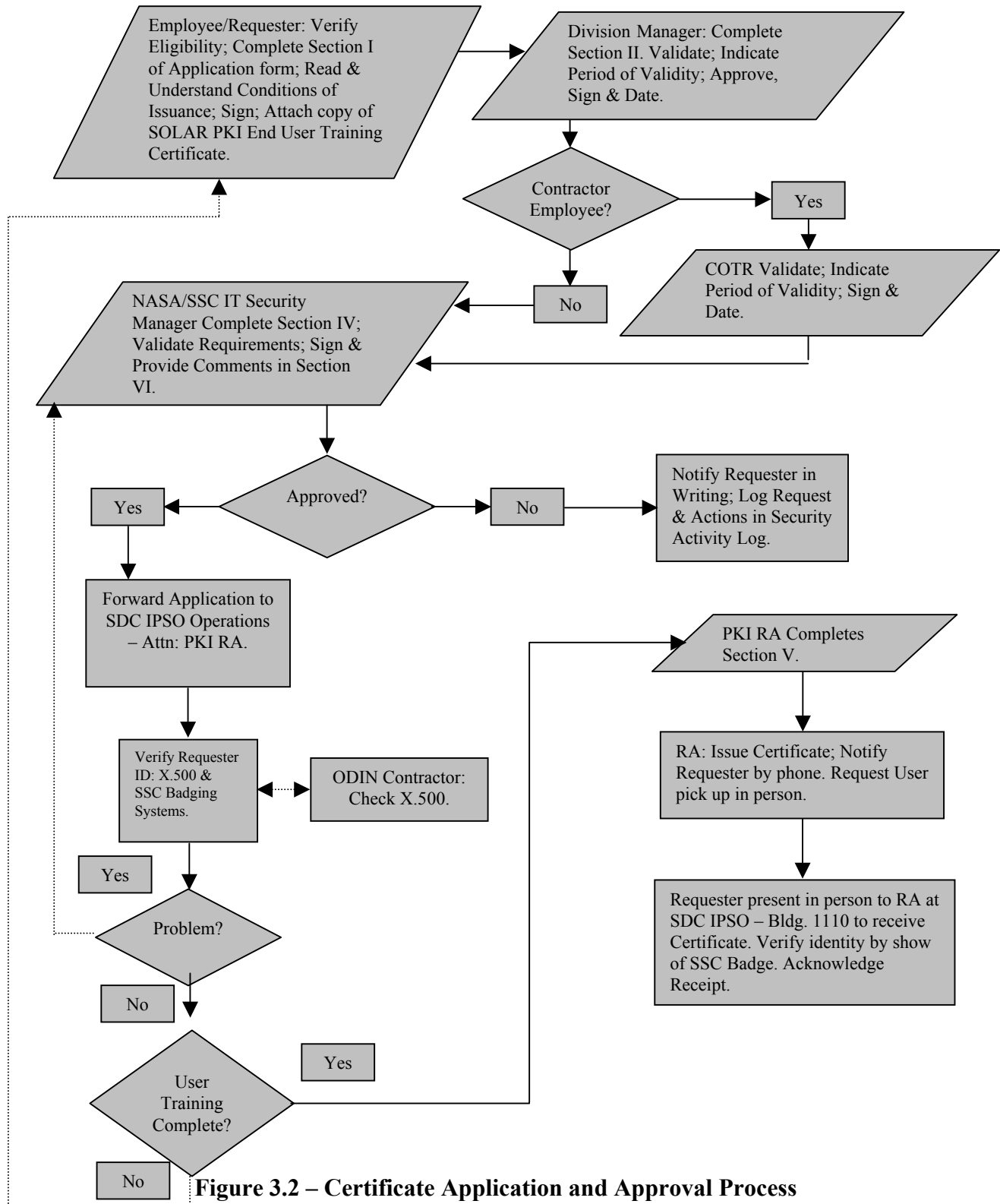


Figure 3.2 – Certificate Application and Approval Process

Stennis Procedural Requirements	SPR 2810.1	Basic
	Number	Rev.
	Effective Date: October 27, 2004	
	Expiration Date: August 3, 2009	
Responsible Office: Center Operations Directorate		Page 15 of 41
SUBJECT: SSC Public Key Infrastructure (PKI) Procedural Requirements		

3.2.4 Certificate Application Procedure

The following procedure is required and used for the Certificate Application process.

1. Requester/Employee: Verify that you satisfy eligibility requirements.
 - (a) You must have a NASA photo ID badge
 - (b) You must have an SSC e-mail account and an entry in the X.500 directory
 - (c) Your PC must satisfy the minimum hardware/software system requirements (See paragraph 3.2.3, Table 1.)
 - (d) You must read and understand the conditions of issuance. (See Note 1. Go to: <http://nasaca.nasa.gov/docs.html>.)
 - (e) You must complete PKI End User training. (See Note 2. Go to: <http://pki.nasa.gov/newuser.html>.)
2. Requester/Employee: Complete Section I of the PKI Certificate Application and Approval Request; read the acknowledgement and declaration of acceptance of the conditions of issuance; sign as the Requester/User; and attach copy of PKI training certificate from SOLAR training system (see Notes 1 and 2). Submit form to Division Manager for requirement validation, approval, and signature.
3. Division Manager: Complete Section II. Validate requirement; indicate period of validity for the Certificate, sign and date. Contractor Manager: Submit form to COTR or Technical Monitor for approval and signature. NASA Manager: Submit to SSC IT Security Manager, Step 5.
4. COTR or Technical Monitor: Complete Section III. Validate requirement, sign, and date. Indicate the validity period for the certificate. Submit form to: NASA/SSC IT Security Manager, Building 1100.
5. NASA/SSC IT Security Manager: Complete Section IV and sign. Approve valid requirement for RA action or reject request for Certificate privileges. Provide comments/explanations in Section VI. If rejected, notify requester in writing. Log request and actions in secure activity Log. Forward approved requests to: SDC IPSO, Bldg. 1110, Attn: PKI RA. Forward information copy to ODIN Contractor for X.500 verification.
6. RA: Complete Section V of request form. Verify requester identity and personal information with X.500 and SSC Badging Systems, sign, and date. Coordinate and resolve problems regarding X.500 with ODIN X.500 Directory Management or NASA/SSC IT Security Manager. Ensure that PKI End User Training has been completed. If not, refer back to requester for completion. Explain actions in Section VI. Log request and actions in secure activity logbook.

Stennis Procedural Requirements	SPR 2810.1	Basic
	Number	Rev.
	Effective Date: October 27, 2004	
	Expiration Date: August 3, 2009	
		Page 16 of 41
Responsible Office: Center Operations Directorate		
SUBJECT: SSC Public Key Infrastructure (PKI) Procedural Requirements		

7. RA: When all actions of item 6 are complete, issue Certificate. Notify requester of Certificate issuance action by phone. Request User to pick up Certificate and Authorization Codes in person at SDC, Building 1110 or hand deliver sealed Certificate issuance letter to User Personally.
8. Requester/User: Verify identity by show of SSC badge to RA. Acknowledge receipt of PKI Certificate and Account Information (see sample in Attachment C) by signing Acknowledgement Memorandum (see sample in Attachment D). Store Certificate information in secure location accessible only to you. Access and install Entrust software per instructions provided in PKI Certificate and Account Information memorandum. Perform online tutorial prior to installation. Establish personal Profile in accordance with the tutorial instructions (see Note 3). Step-by-step instructions for creating a profile for the first time are also provided at <http://pki.nasa.gov/training.html>.

Note 1: All requesters must read/understand the NASA PKI X.509 Certificate Policy and Certification Practice Statement and acknowledge/accept conditions of issuance. Requesters must agree to the terms of the NASA PKI Subscriber Agreement. (NASA PKI documents are published on the Internet at <http://nasaca.nasa.gov/docs.html>. SSC PKI procedures and guidelines are provided in SPR 2810.1.) The Subscriber Agreement will become effective on the date you submit your Certificate application to the SSC PKI Registration Authority [RA].

Note 2: Applicants must complete PKI End-User training prior to use of a PKI Certificate. The training certificate should be submitted along with the application. PKI Certificates will not be issued until training is complete. Access to the SOLAR training site as well as useful information on getting started with PKI is available at: <http://pki.nasa.gov/newuser.html>. Select **PKI Enduser Training** to go to the SOLAR web page. Request a User ID then select **Public Key Infrastructure** from the list of available on-line training courses. NASA SOLAR training is also accessible at <https://solar.msfc.nasa.gov:443/>.

Note 3: Instructions for software access and installation will be provided when the PKI Certificate is issued. Upon initial access to the Entrust software for installation, Users shall complete the included tutorial before beginning the actual installation process and setting up the User Profile. Step-by-step instructions for creating a profile for the first time are also provided at <http://pki.nasa.gov/training.html>.

3.3 PKI Certificate Revocation and Suspension/Disabling Process

The Certificate Revocation and Suspension/Disabling process is used to permanently revoke or temporarily suspend/disable a User's PKI access privileges for various reasons. A flowchart of the process is presented in Figure 3.3.

To revoke, suspend, or disable User privileges, Requester/Users must complete the NASA/SSC PKI Certificate Revocation and Suspension Disabling Request form available under "Forms" on

Stennis Procedural Requirements	SPR 2810.1	Basic
	Number	Rev.
	Effective Date: October 27, 2004	
	Expiration Date: August 3, 2009	
Responsible Office: Center Operations Directorate		Page 17 of 41
SUBJECT: SSC Public Key Infrastructure (PKI) Procedural Requirements		

the SSC Intranet internal home page. Depending upon the circumstances of the request, an immediate report and notification to the C-ITSM and the RA may also be required in accordance with instructions provided in this document.

Complete process instructions are provided with the form. The form must be filled out legibly and completely. Requesters should read and follow all instructions. Requesters are cautioned that misuse of PKI processes may constitute grounds for termination of privileges, administrative action, and/or civil or criminal prosecution. Any form lacking information will be disregarded.

3.3.1 When to Use Revocation and Suspension/Disabling Process

3.3.1.1 Revocation

Certificates will be revoked when a Certificate is no longer trusted for any reason. This includes encryption and/or verification Certificates for End Users, RA Administrators, and PKI Security Officers. Loss of trust includes but is not limited to:

1. Dismissal or suspension for cause;
2. Compromise/suspected compromise of private key and/or User password and profile;
3. Change in Requester's/User's role (e.g., organizational change between Centers) or permissions;
4. Termination of employment; and
5. Failure of Requester/User to meet specified obligations under the NPR and relevant policies.

Key compromise, suspected compromise or dismissal for cause is provocation for immediate revocation of User access. These events are classified as security incidents and will be handled in accordance with SSC Security Incident/Investigative procedures. Reports of incidents of key compromise, suspected compromise, or dismissal for cause MUST be placed within 1 hour of the detection of the compromise or suspected compromise. To report such cases or incidents, phone or e-mail the SSC IT Security Manager detailing reasons and circumstances or phone the SSC PKI RA at ext. 8-2116. Follow up with submission of an approved Revocation Request form. The IT Security Manager will validate immediate requirements and coordinate revocation with the PKI RA.

Requests for revocation for other reasons MUST be placed within 24 hours of the change.

Stennis Procedural Requirements	SPR 2810.1	Basic
	<i>Number</i>	<i>Rev.</i>
	Effective Date: October 27, 2004	
	Expiration Date: August 3, 2009	
		Page 18 of 41
Responsible Office: Center Operations Directorate		
SUBJECT: SSC Public Key Infrastructure (PKI) Procedural Requirements		

3.3.1.2 Suspension/Disabling

Certificates may be suspended and disabled for such circumstances as when a User goes on leave or is no longer a part of the domain. Disabled User accounts may be re-enabled at a later time. Re-application is required to re-enable. Notification to Suspend/Disable a User Certificate MUST be made as soon as the requirement is known or within 24 hours of identification of the requirement or change.

3.3.1.3 Accidental Key Compromise

An immediate report of any key compromise situation must be filed with the PKI RA at ext. 8-2116 giving the circumstances of the compromise. See paragraph 3.3.1.1. If the compromise is accidental on the part of the User/Requester, no further notification action is required. The RA will rescind access. Users must follow up with a request for Key Recovery to regain access.

3.3.2 Who May Request

Revocation or suspension/disabling of a User's or an end-entity's Certificate may be requested by:

1. Any responsible personnel (i.e., requesters other than the User);
2. End Users;
3. NASA Office of Investigative Services;
4. IPSO IT Security Officer;
5. RA Administrator;
6. PKI RA;
7. User's Management; or
8. SSC IT Security Manager.

3.3.3 Reinstatement of Revoked Privileges

Reinstatement of a revoked Certificate is permitted only under specific circumstances. Re-application with administrative review and determination is required. Reinstatement may be permitted for the following situations:

1. Organizational changes within NASA that result in Distinguished Name changes affecting several employees; or
2. Revocations not the result of a key compromise and the User is temporarily unavailable to present him/herself in person.

Stennis Procedural Requirements	SPR 2810.1	Basic
	Number	Rev.
	Effective Date: October 27, 2004	
	Expiration Date: August 3, 2009	
	Page 19 of 41	
Responsible Office: Center Operations Directorate		
SUBJECT: SSC Public Key Infrastructure (PKI) Procedural Requirements		

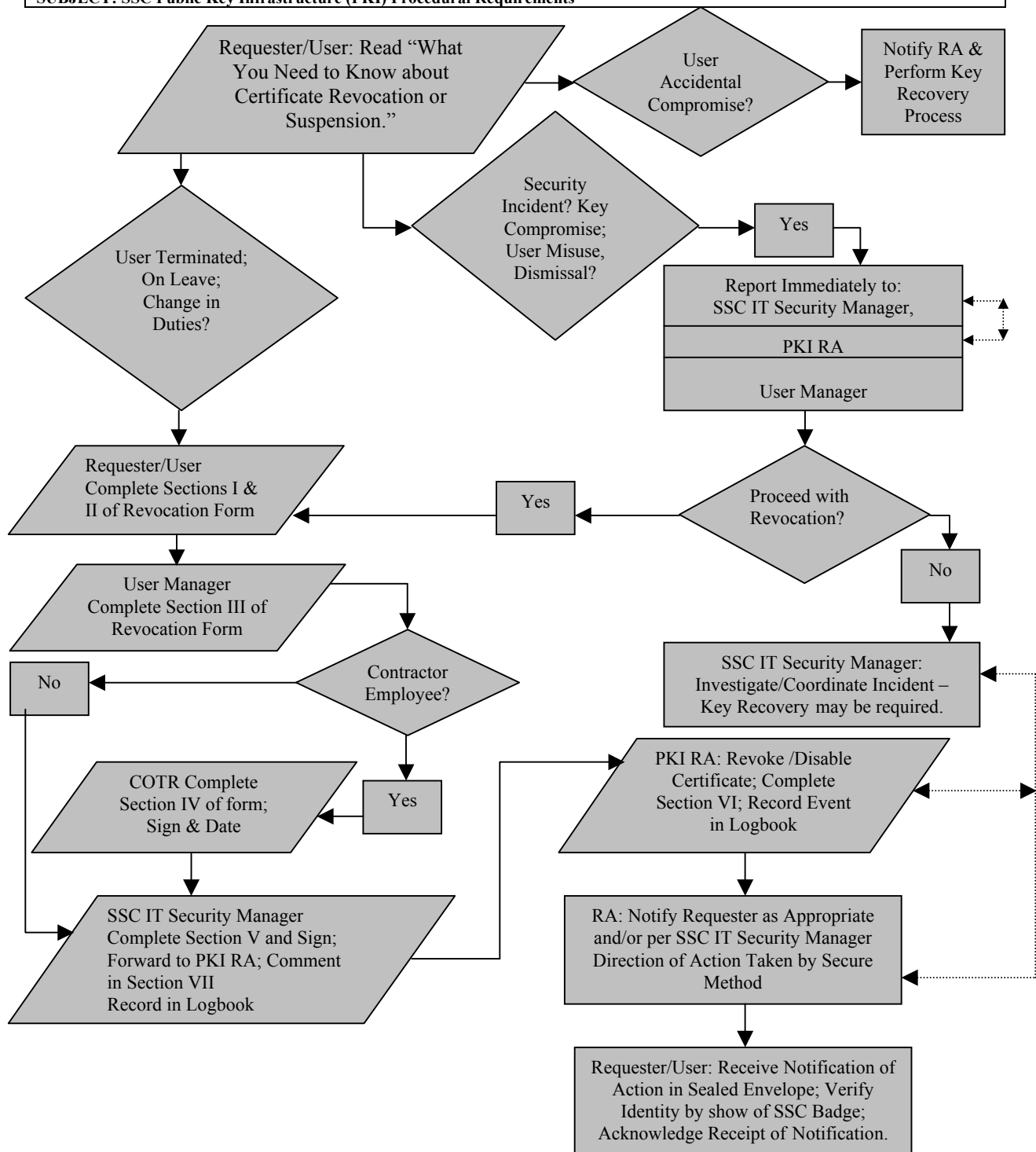


Figure 3.3 – Revocation and Suspension/Disabling Process

Stennis Procedural Requirements	SPR 2810.1	Basic
	Number	Rev.
	Effective Date: October 27, 2004	
	Expiration Date: August 3, 2009	
Responsible Office: Center Operations Directorate		Page 20 of 41
SUBJECT: SSC Public Key Infrastructure (PKI) Procedural Requirements		

3.3.4 Revocation and Suspension/Disabling Procedure

The following procedure is required and used for the Revocation and Suspension/Disabling process:

1. Requester: Read "What You Need to Know about Certificate Revocation and Suspension" on the Revocation and Suspension/Disabling Request form and per guidance in this document. Notify NASA/SSC IT Security Manager and/or SSC PKI RA by phone (ext. 8-2116) or e-mail of serious incident and immediate revocation requirement (e.g., key compromise, suspected compromise, dismissal for cause) as appropriate. Also notify the User's management if an immediate revocation action is requested. Follow up with submittal of Revocation and Suspension/Disabling Request form as required by the circumstances of the triggering event. Note: Someone other than the Certificate User may be the requester for the process.
2. Requester/User: Complete Section I of the request form. Indicate the type of action requested (e.g., suspend/disable for temporary requirements; revoke if serious incident; delete if the User no longer needs or is terminating employment). Sign as the Requester. Provide detailed reason for action requested. Indicate period of suspension/disabling as applicable.
3. Requester/User: Complete Section II of the form providing Certificate User information. Submit form to User Management for notification/approval and signature. If someone other than the Certificate User is requesting the action, all of the requested User information may not be known. If not the Certificate User, Requesters should provide as much information as possible.
4. User Management: Complete Section III of request form and sign. Contractor: Submit form to COTR or Technical Monitor for notification, approval, and signature. NASA Manager: Submit form to IT Security Manager, Step 6.
5. COTR or Technical Monitor: Complete Section IV of request form and sign. Submit form to NASA/SSC IT Security Manager, Building 1100.
6. SSC IT Security Manager: Complete Section V of request form and sign. Indicate action taken and, as appropriate to circumstances, the date User and/or User Management is notified of suspension or revocation action. Provide explanatory comments on notifications and actions in Section VII. Record the events and actions in logbook. Submit form to SDC IPSO, Bldg. 1110, Attn: PKI RA.
7. RA: Complete Section VI of request form and sign. Indicate action taken and date of action; disable/suspend or revoke Certificate per direction, and record event in logbook.

Stennis Procedural Requirements	SPR 2810.1	Basic
	Number	Rev.
	Effective Date: October 27, 2004	
	Expiration Date: August 3, 2009	
Responsible Office: Center Operations Directorate		Page 21 of 41
SUBJECT: SSC Public Key Infrastructure (PKI) Procedural Requirements		

Indicate period of suspension as applicable. Indicate notification date to SSC IT Security Manager of immediate revocation requirements if reported directly to RA.

8. RA: Notify Requester (and/or User) as appropriate to circumstances and/or per SSC IT Security Manager direction of action taken by secure method. (See sample letter template in Attachment E.)
9. Requester/User: Receive notification of action taken via sealed envelope or other secure method. Verify identity by show of SSC badge. Acknowledge receipt of information by signing and returning memorandum of acknowledgement (Attachment F).

3.4 Key Recovery Process

The Key Recovery process is used to revise a User's profile data and reassign new key pairs for accessing previously encrypted data. The User's current key pairs are disabled. The Key Recovery process may be invoked for security or legal reasons, Certificate Revocations or Suspensions, as well as for business continuity purposes to recover and view previously encrypted data. Requests may be made by Certificate Users or by other requesting personnel without the User's consent. Non-emergency requests for Key Recovery will typically be completed within 48 hours. In other cases, Key Recovery will be performed depending upon the situation.

To initiate a Key Recovery process, Requester/Users must complete the NASA/SSC PKI Certificate Key Recovery Request form available under "Forms" on the SSC Intranet internal home page. Depending upon the circumstances of the request, an immediate report and notification to the SSC IT Security Manager and the PKI RA may also be required in accordance with instructions provided in this document.

Complete process instructions are provided with the form. The form must be filled out legibly and completely. Requesters should read and follow all instructions. Requesters are cautioned that misuse of PKI processes may constitute grounds for termination of privileges, administrative action, and/or civil or criminal prosecution. Any form lacking information will be disregarded. A flowchart of the process is presented in Figure 3.4.

3.4.1 Who May Request

Key Recovery actions may be initiated by:

1. End Users;
2. User's Management;
3. SSC IT Security Manager;
4. Law Enforcement Agencies/Court Orders; or
5. Other Requesters with justifiable need or security concerns.

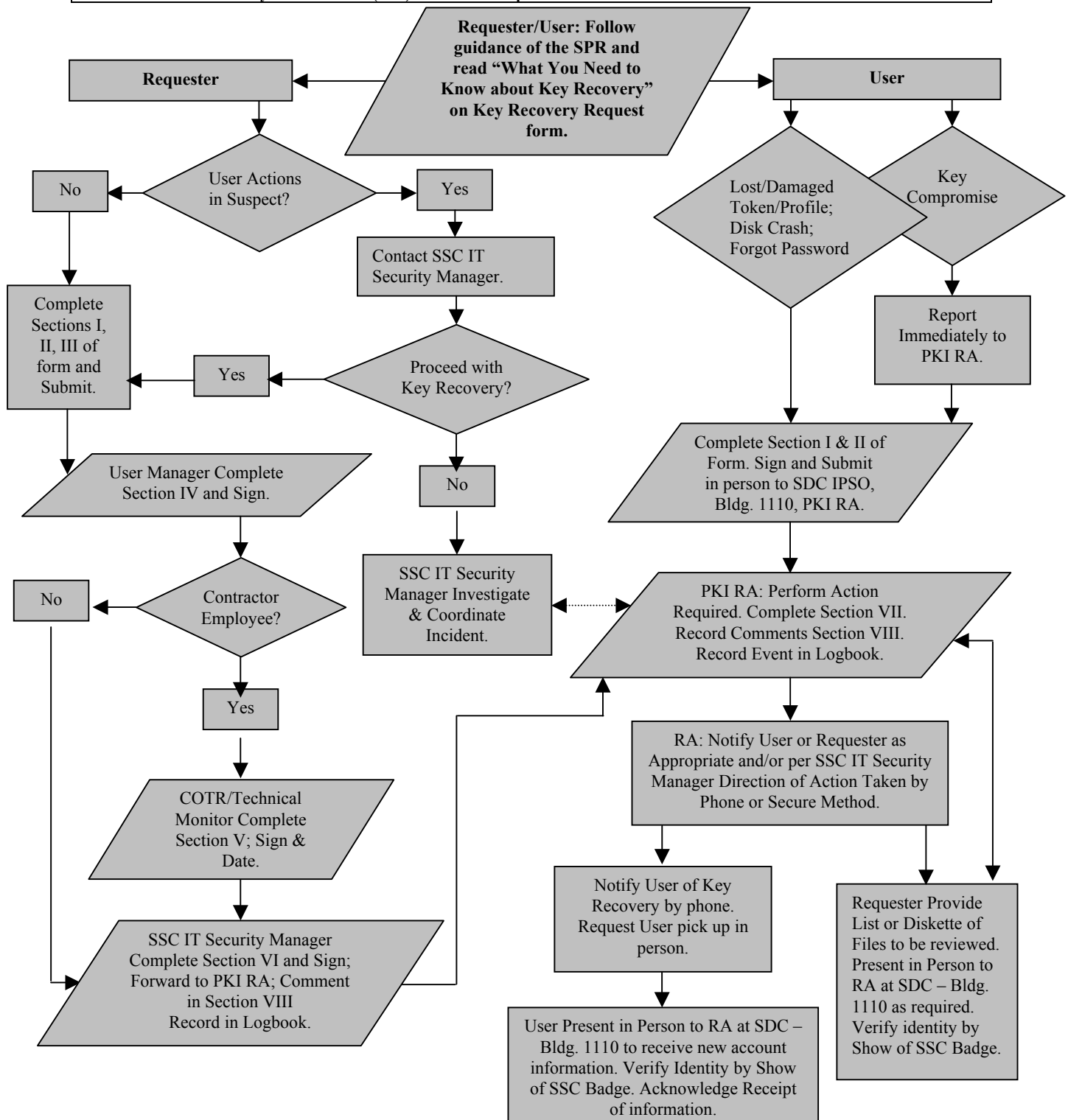


Figure 3.4 – Key Recovery Process

3.4.2 When to Use the Key Recovery Process

Stennis Procedural Requirements	SPR 2810.1	Basic
	<i>Number</i>	<i>Rev.</i>
	Effective Date: October 27, 2004	
	Expiration Date: August 3, 2009	
Responsible Office: Center Operations Directorate		Page 23 of 41
SUBJECT: SSC Public Key Infrastructure (PKI) Procedural Requirements		

3.4.2.1 User Requests for Key Recovery

Examples for User requested Key Recovery include but are not necessarily limited to, the reasons below. To protect against unauthorized requests, User's should personally submit written, signed requests and validate their identity upon submittal.

1. User forgets Password;
2. User loses or damages a PKI profile file;
3. User loses or damages a security token (PCMCIA card);
4. User suspects keys have been compromised; or
5. User accidentally compromises his/her keys.

An immediate report of any key compromise situation must be filed with the PKI RA giving the circumstances of the compromise. The PKI RA will suspend accessibility to a User's files. If the compromise is accidental on the part of the User, no further notification is required but the User must follow up with submission of a written Key Recovery Request. Access will be renewed with reassignment of new key pairs through the Key Recovery process. Key Recovery actions must be performed and witnessed by two certified RA personnel. The PKI RA will provide new access instructions to the User through secure methods.

3.4.2.2 Non-User-Consent Key Recovery

Key Recovery actions may be initiated without User consent for investigative or business continuity purposes. Actions may or may not be disclosed to the User. Examples for Key Recovery without User consent include but are not necessarily limited to:

1. User leaves the organization and management needs to recover and decrypt the User's files for business continuity;
2. User's actions are in question by SSC IT Security Manager and User's files need to be reviewed; or
3. User's actions are in question by an external law enforcement agency and User's files need to be reviewed.

To protect Users from unauthorized access to their files, all requests for Key Recovery submitted without the User consent must be approved through a formal and official written notification and approval process. In certain situations, a Court Order for Key Recovery will constitute written approval. Key Recovery actions must be performed and witnessed by two certified RA personnel.

Stennis Procedural Requirements	SPR 2810.1	Basic
	Number	Rev.
	Effective Date: October 27, 2004	
	Expiration Date: August 3, 2009	
Responsible Office: Center Operations Directorate		Page 24 of 41
SUBJECT: SSC Public Key Infrastructure (PKI) Procedural Requirements		

3.4.2.3 Should Key Recovery Be Performed?

The decision to perform a Key Recovery without User consent should be made with discretion by the Requester, in consideration of the particular circumstances. When a User discovers a change in accessibility, the PKI RA may be contacted for assistance. Requesters should assess the impact of disclosure to the User and, depending upon circumstances may choose not to perform a Key Recovery. Security issues and concerns should be reported to and coordinated with the SSC IT Security Manager for determination of appropriate course of action. In choosing Key Recovery, Requesters must provide instructions on whether or not the Key Recovery action is to be disclosed and what specific information may or may not be provided to the User.

3.4.3 Key Recovery Procedure

The following procedure is required and used for the Key Recovery process:

1. Requester/User: Read "What You Need to Know about Key Recovery" on the instruction sheet of the NASA/SSC PKI Certificate Key Recovery Request form and follow the guidance provided in this document.
2. Requester/User: Complete Section I of request form. Indicate who is making the request. Someone other than the User may be making the request. Check reason box and provide detailed reason for action. If the request reason is a suspected Key Compromise, see Note below and also follow procedure for incident reporting.
3. Requester/User: Complete Section II of the request form, providing Certificate User information. If User is submitting request, she/he should sign in the approval block and go to Step 4. If the Requester is someone other than the Certificate User, and the request is being submitted without the User's knowledge, provide as much User information as possible and go to Step 5 and complete Section III.
4. User: Submit form in person to PKI RA, SDC, Building 1110. No other approvals are required. Upon arrival at Building 1110, call ext. 8-2116 to request RA escort for entry into the facility and presentation of request. Verify identity by show of SSC Badge.
5. Requester: Contact the SSC IT Security Manager and/or PKI RA to determine course of action. Complete Section III of request form and sign. Identify the person(s) to be responsible for viewing and controlling recovered files. Identify files to be viewed (all or specific). Provide instruction as to whom disclosure of the Key Recovery action should be made and what information is to be provided. Submit form to User's management for notification and approval of requested action. If applicable, Requesters may be requested to supply a diskette containing the User's files to be viewed during the scheduled Key Recovery.

Stennis Procedural Requirements	SPR 2810.1	Basic
	Number	Rev.
	Effective Date: October 27, 2004	
	Expiration Date: August 3, 2009	
Responsible Office: Center Operations Directorate		Page 25 of 41
SUBJECT: SSC Public Key Infrastructure (PKI) Procedural Requirements		

6. User Management: Complete Section IV of form acknowledging notification and sign. Contractor Manager: Submit form to COTR or Technical Monitor for notification/approval and signature. NASA Manager: Submit form to NASA/SSC IT Security Manager, Step 8.
7. COTR or Technical Monitor: Complete Section V of request form acknowledging notification and sign. Submit form to: NASA/SSC IT Security Manager, Building 1100.
8. SSC IT Security Manager: Validate requirement and sign approval in Section VI of request form. Provide explanatory comments on notifications and actions in Section VIII. Record events and actions in logbook. Submit form to: SDC IPSO, Bldg. 1110, Attn: PKI RA.
9. RA: Perform actions required. Complete Section VII of request form and sign (two signatures required). Indicate Date of Action, and record event in logbook. Indicate the date the SSC IT Security Manager was notified as applicable to circumstances. Provide explanatory comments of actions and notifications in Section VIII.
10. RA: Notify User and/or Requester as appropriate to circumstances of request by phone or other secure method and/or per SSC IT Security Manager direction of action taken.
 - (a) Request User to pick up new account information in person.
 - (b) Request other Requester to provide list or diskette of files for review by Key Recovery action.
11. User: Present in person to PKI RA at SDC, Bldg. 1110. Verify identity by show of SSC badge upon delivery. Acknowledge receipt of new account information.
12. Requester: Supply list or diskette of files to be reviewed. Present in person to PKI RA at SDC, Bldg. 1110 as required. Verify identity by show of SSC Badge.

Note: Key compromise, suspected compromise, or dismissal for cause is provocation for immediate revocation of User Certificate. These events are classified as security incidents and will be handled in accordance with SSC Security Incident/Investigative procedures.

Reports of incidents of key compromise, suspected compromise, or dismissal for cause MUST be placed within 1 hour of the detection of the compromise or suspected compromise. To report such cases or incidents, phone or e-mail the SSC IT Security Manager detailing reasons and circumstances or phone the SSC PKI RA at ext. 8-2116. Follow up with submission of approved Revocation and/or Key Recovery request form. The SSC IT Security Manager will validate immediate requirements and coordinate revocation and key recovery requirements with the PKI RA.

3.5 Help Desk – Ext. 2525

Stennis Procedural Requirements	SPR 2810.1	Basic
	<i>Number</i>	<i>Rev.</i>
	Effective Date: October 27, 2004	
	Expiration Date: August 3, 2009	
		Page 26 of 41
Responsible Office: Center Operations Directorate		
SUBJECT: SSC Public Key Infrastructure (PKI) Procedural Requirements		

For assistance in resolution of PKI User support questions and problems, Users should call the Help Desk at ext. 8-2525 Option 4. Responsibilities for resolution of User questions are divided between the SDC PKI RA, the SSC ODIN Contractor, and the PKI Support Group at ARC. The Help Desk will field all Help Desk calls and provide the appropriate support and/or route requests to the appropriate resource for resolution. Help Desk support is available during normal workday hours at ext. 8-2525 Option 4.

The ODIN Contractor has primary responsibility for provision of resources and support for:

1. Maintenance and configuration of and access to the Entrust software;
2. Entrust software general maintenance (bug fixes, patches, new releases);
3. General user problems such as computer lockups when initializing the application; and
4. Resolution of problems related to relationship between the Entrust software and X.500 Directory.

The SDC PKI RA will provide support to resolve PKI administrative problems and questions regarding Certificate issuance, enabling, revoking, key recovery, reports, etc. Questions specifically related to these issues may be submitted directly to the SSC PKI RA at ext. 8-2116 or by calling the Help Desk at 8-2525 Option 4. The PKI RA will contact the NASA PKI Support Group at ARC to gain resolution to problems as needed.

The NASA PKI Support Group at ARC is responsible for the overall administration, maintenance, and operations of the NASA PKI system. The PKI Support Group is responsible for:

1. Coordinating and resolving issues relative to the Entrust software;
2. Coordinating and distributing software bug fixes, upgrades, patches, etc.; and
3. Resolution of problems related to Entrust software operation (e.g., troubles sending encrypted messages).

3.6 RA Facility Security and Access

The SSC Information Processing Service Organization (IPSO) is the Stennis Data Center located in Building 1110 and is considered a High-Security Zone. Entry into the building as well as the SDC/PKI operations area (Room 101, computer room) is controlled via card key entry. The SDC Operations Manager controls and issues key cards and maintains a log of personnel to whom cards are issued. Personnel must sign the log indicating receipt of a key card and acknowledge understanding of the procedures regarding access to the building and the SDC IPSO. Personnel must justify a need for issuance of a key card. Employees are required to notify the SDC Operations Manager when access requirements change and to immediately return issued key cards. The Operations Manager maintains the Key Card log for examination by the IPSO ITSO. Security issues are coordinated with the IT Security Liaison, the NASA Office of Chief Information Officer, and the SSC IT Security Manager.

Stennis Procedural Requirements	SPR 2810.1	Basic
	<i>Number</i>	<i>Rev.</i>
	Effective Date: October 27, 2004	
	Expiration Date: August 3, 2009	
Page 27 of 41		
Responsible Office: Center Operations Directorate		
SUBJECT: SSC Public Key Infrastructure (PKI) Procedural Requirements		

Visitors to the building must be “passed” into the building by a valid building occupant. All visitors to the building must register on a manual entry log. The visitor’s name, organization, the time and date of entry and exit, person being called upon, and reason for visit must be given in the register.

Visitors to the SDC IPSO must be escorted by an authorized person and must also sign in and out on the “SDC Computer Room Visitor’s Log” located in the computer room. All visitors will indicate the organization they represent, date and time of entry/exit, and reason for visit. Authorized IPSO personnel will escort all visitors or any individual that has not been issued a key card.

SDC operations personnel and PKI RA personnel are responsible for insuring that visitors remain in designated secure areas of the area. Visitors are not permitted to touch any equipment or view any data other than that required for purpose of the visit.

Any unauthorized access or attempted access to the building and/or the SDC computer room shall be reported to the IPSO Information Technology Security Officer (IPSO ITSO) and SDC Operations Manager immediately. Unauthorized persons found in the building or computer room will be escorted out immediately. The name and organization of the person and reason for the entry should be determined. Re-entry will be permitted only upon valid justification and proper escort and registration. The IPSO ITSO will coordinate and resolve security issues with the TSC IT Security Liaison and the SSC IT Security Manager.

Personnel requiring access to the SDC for the conduct of valid PKI RA purposes should phone ext. 8-2116 to announce visit and request escort.

Complete operating procedures for the IPSO are maintained by the SDC.

3.7 Software Distribution and Control

Entrust software used for the PKI certificate process is controlled by the PKI RA. The number of PKI Certificates and Entrust licenses available for PKI use is limited. Software is maintained by the SSC ODIN Contractor. The PKI RA provides access instructions for installation upon completion of the Certificate application process.

Stennis Procedural Requirements	SPR 2810.1	Basic
	<i>Number</i>	<i>Rev.</i>
	Effective Date: October 27, 2004	
	Expiration Date: August 3, 2009	
Responsible Office: Center Operations Directorate		Page 28 of 41
SUBJECT: SSC Public Key Infrastructure (PKI) Procedural Requirements		

3.7.1 Entrust Software Training and Installation

PKI Certificate applicants must complete PKI End User training prior to Certificate issuance and complete the Entrust software tutorial at the time of software installation. Access to the software and its tutorial will be provided upon approval and issuance of the PKI Certificate. Users will access and install the Entrust software following instructions provided by the PKI RA. End Users should not attempt to access, download, or use the Entrust software from any on-line resources or other sources other than that access specifically provided by the SSC PKI RA. Non-authorized access is prohibited.

3.7.2 Software Removal and Account Terminations

The SSC IT Security Team and/or ODIN Contractor will remove any Entrust software from the computers of unauthorized Users and from computers of terminating personnel. Use of the software may not be passed from an outgoing employee to an incoming replacement. Entrust software will be removed from any computer transferring User ownership or any computer removed from service by the ODIN Contractor.

Terminating employees or those changing responsibilities must notify the PKI RA by submission of a NASA/SSC Certificate Revocation and Suspension/Disabling Request. Employee managers are obligated to ensure the submission of an order to the PKI RA and/or ODIN Contractor for disposition of IT resources including Entrust software for terminating personnel or for those whose requirements have changed.

The SDC is automatically notified by e-mail of all NASA and NASA Contractor personnel terminations. The PKI RA will check these termination notices against user lists and will automatically disable any user accounts for terminating personnel. To gain access to the previously encrypted files or records of terminated personnel, managers of terminated personnel must submit a Key Recovery Request.

3.7.3 Entrust Software Maintenance

The ODIN Contractor will install software bug fixes, patches, and new releases for the Entrust software upon notification from and in coordination with the SSC PKI RA or the Ames Research Center (ARC) PKI Manager or Support Group.

3.8 Documentation and Data Control

Documentation generated in the course of PKI RA activity specifically includes:

1. Personnel identification and authentication information;
2. Key Certificate requests and approvals or rejections;
3. Certificate suspension approvals;

Stennis Procedural Requirements	SPR 2810.1	Basic
	<i>Number</i>	<i>Rev.</i>
	Effective Date: October 27, 2004	
	Expiration Date: August 3, 2009	
Responsible Office: Center Operations Directorate		Page 29 of 41
SUBJECT: SSC Public Key Infrastructure (PKI) Procedural Requirements		

4. Certificate revocation approvals;
5. Key recovery approvals; and
6. Activity logbooks.

Other ancillary records also may be generated or compiled during administrative and operations activities. These may include e-mail, reports, letters, notices, and memorandums or copies of such.

All documentation and records of PKI activities will be maintained and retained for a minimum period of 5 years. Disposition will be in accordance with NPR 1441.1, NASA Records Retention Schedules (NRRS), Schedule 2, AFS number 2810.

To protect the privacy of personal information contained in the records and ensure the security of critical sensitive data, all documentation will be stored in secure files or systems. Access to personal information will be limited to responsible SSC PKI program personnel and SSC security officers on an as needed basis. Key recovery transactions and recovery of previously encrypted data must be approved by the SSC IT Security Manager and witnessed by two RA operations personnel.

Stennis Procedural Requirements	SPR 2810.1	Basic
	<i>Number</i>	<i>Rev.</i>
	Effective Date: October 27, 2004	
	Expiration Date: August 3, 2009	
Responsible Office: Center Operations Directorate		Page 30 of 41
SUBJECT: SSC Public Key Infrastructure (PKI) Procedural Requirements		

APPENDICES

Stennis Procedural Requirements	SPR 2810.1	Basic
	<i>Number</i>	<i>Rev.</i>
	Effective Date: October 27, 2004	
	Expiration Date: August 3, 2009	
Responsible Office: Center Operations Directorate		Page 31 of 41
SUBJECT: SSC Public Key Infrastructure (PKI) Procedural Requirements		

Appendix A: Acronyms

ARC	Ames Research Center
CA	Certification Authority
CCS	Center Chief of Security
CIO	Chief Information Officer
C-ITSM	Center IT Security Manager
CP	Certificate Policy
COTR	Contracting Officer's Technical Representative
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DN	Distinguished Name
IPSO	Information Processing Service Organization (Stennis Data Center [SDC] formerly PSCS)
IPSO ITSO	Information Processing Service Organization Information Technology Security Officer
IT	Information Technology
ITS	Information Technology Services Contract
ITU	International Telecommunications Union
NASA	National Aeronautics and Space Administration
NASIRC	NASA Automated Systems Incident Response Capability
NPD	NASA Policy Directive
NPR	NASA Procedures and Requirements
ODIN	Outsourcing Desktop Initiative (IT Services Contractor)
OID	Object Identifier
PA	Policy Authority
PKI	Public Key Infrastructure
PSCS	SSC Program Support Computer System
RA	Registration Authority
RASA	Registration Authority System Administrator
SDC	Stennis Data Center (SSC Information Processing Service Organization, formerly PSCS)
SOLAR	Site for On-Line Learning and Resources
SPR	Stennis Procedures and Requirements
SSC	Stennis Space Center

Stennis Procedural Requirements	SPR 2810.1	Basic
	Number	Rev.
	Effective Date: October 27, 2004	
	Expiration Date: August 3, 2009	
Responsible Office: Center Operations Directorate		Page 32 of 41
SUBJECT: SSC Public Key Infrastructure (PKI) Procedural Requirements		

Appendix B: Definitions

Activation Data. Private data, other than keys, that are required to access cryptographic modules.

Authority Revocation List (ARL). A list of revoked CA certificates. An ARL is a CRL for CA cross certificates.

Certificate. The public key of a User, together with some other information, rendered unforgeable by digitally signing it with the private key of the certification authority that issued it. The certificate format is in accordance with ITU-T Recommendation X.509.

Certificate Revocation List (CRL). A list of revoked certificates that is created and signed by the same CA that issued the certificates. A certificate is added to the list if it is revoked (e.g., because of suspected key compromise). In some circumstances the CA may choose to split a CRL into a series of smaller CRL's.

Certification Authority. An authority trusted by one or more Users to issue and manage X.509 public key certificates and CRL's.

Digital Signature. The result of a transformation of a message by means of a cryptographic system using keys such that a person who has the initial message can determine:

- (a) Whether the transformation was created using the key that corresponds to the signer's key; and
- (b) Whether the message has been altered since the transformation was made.

Directory. A directory system that conforms to the ITU-T X.500 series of recommendations.

Employee. An employee is any person employed by NASA or NASA Contractor.

End Entity. An Entity that uses the keys and certificates created within the PKI for purposes other than the management of the aforementioned keys and certificates. An End Entity may be a Subscriber, a Relying Party, a device, or an application.

Entity. Any autonomous element within the Public Key Infrastructure. This may be a CA, RA, or an End Entity.

High-security Zone. An area to which access is controlled through an entry point and limited to authorized appropriately screened personnel and properly escorted visitors. High-Security Zones should be separated by a perimeter. High-Security Zones are monitored 24 hours a day and 7 days a week by security staff, other personnel, or electronic means.

Issuing CA. In the context of a particular certificate, the issuing CA is the CA that signed and issued the certificate.

Stennis Procedural Requirements	SPR 2810.1	Basic
	Number	Rev.
	Effective Date: October 27, 2004	
	Expiration Date: August 3, 2009	
Responsible Office: Center Operations Directorate		Page 33 of 41
SUBJECT: SSC Public Key Infrastructure (PKI) Procedural Requirements		

MD5. One of the message digest algorithms developed by RSA Data Security Inc.

Object Identifier. (OID) The unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class.

Organization. A department, agency, corporation, partnership, trust, joint venture, or other association.

Operational Authority. Personnel responsible for the overall operation of a NASA PKI CA. Their responsibility covers areas such as staffing, finances, and dispute resolution. The Operational Authority role does not require an account on the CA workstation.

Public Key Infrastructure (PKI). A structure of hardware, software, people, processes and policies that uses Digital Signature technology to provide Relying Parties with a verifiable association between the public component of an asymmetric key pair with a specific Subscriber.

Policy Authority. A NASA body responsible for setting, implementing, and administering policy decisions regarding CP's and CPS's throughout the NASA PKI.

Registration Authority (RA). An Entity that is responsible for the identification and authentication of certificate Subscribers before certificate issuance, but does not actually sign or issue the certificates (i.e., a RA is delegated certain tasks on behalf of a CA).

Relying Party. A person who uses a certificate signed by a NASA PKI CA to authenticate a digital signature or to encrypt communications to the certificate subject, and is a Subscriber of a NASA PKI CA or a PKI which is cross certified with the NASA PKI.

Sponsor. A Sponsor in the NASA PKI is the NASA department or civil servant that has nominated that a specific individual or organization be issued a certificate (e.g., for an employee this may be the employee's manager). The Sponsor is responsible for informing the CA or RA if the relationship with the Subscriber is terminated or has changed such that the certificate should be revoked or updated.

Subscriber. An individual or organization whose public key is certified in a public key certificate. In the NASA PKI this could be a civil servant, or a NASA Contractor. Subscribers may have one or more certificates from a specific CA associated with them; most will have at least two active certificates - one containing their Digital Signature verification key; the other containing their Confidentiality encryption key.

Stennis Procedural Requirements	SPR 2810.1	Basic
	<i>Number</i>	<i>Rev.</i>
	Effective Date: October 27, 2004	
	Expiration Date: August 3, 2009	
Responsible Office: Center Operations Directorate		Page 34 of 41
SUBJECT: SSC Public Key Infrastructure (PKI) Procedural Requirements		

ATTACHMENTS

Stennis Procedural Requirements	SPR 2810.1	Basic
	<i>Number</i>	<i>Rev.</i>
	Effective Date: October 27, 2004	
	Expiration Date: August 3, 2009	
		Page 35 of 41
Responsible Office: Center Operations Directorate		
SUBJECT: SSC Public Key Infrastructure (PKI) Procedural Requirements		

Attachment A: SSC PKI Key Personnel and Critical Contacts

SSC RA Administrator (Operational Authority):

James Cluff
SSC IT Security Manager
Center Operations Directorate
John C. Stennis Space Center, MS 39529

RA Authorities:

Mike C. Bounds
John C. Stennis Space Center, MS 39529

Contractor IT Security Liaison:

Hillman Holley
Information Services Directorate
John C. Stennis Space Center, MS 39529

NOTE: This contact list is for illustration purposes. Contact the SSC IT Security Manager for current list.

Stennis Procedural Requirements	SPR 2810.1	Basic
	<i>Number</i>	<i>Rev.</i>
	Effective Date: October 27, 2004	
	Expiration Date: August 3, 2009	
		Page 36 of 41
Responsible Office: Center Operations Directorate		
SUBJECT: SSC Public Key Infrastructure (PKI) Procedural Requirements		

Attachment B: Nondisclosure Agreement

EXAMPLE ONLY

As an employee of _____, performing services at the NASA Stennis Space Center, I recognize that I will be required to perform certain activities which may expose me to NASA or industry sensitive information or material which may be proprietary to NASA or companies involved with these activities. Access to or possession of such information or material may occur through operational requirements, meetings, visits to other facilities, during data entry, etc. which are required as part of my assigned task. Under these circumstances, I agree not to disclose such information or material to any unauthorized parties including personnel and management.

I have read and understand the policies pertaining to nondisclosure or conflict of interest and I understand that unauthorized disclosure of proprietary or competitive sensitive data will result in severe disciplinary action and possible dismissal.

Employee Name

Signature

Date

Manager

Signature

Date

Stennis Procedural Requirements	SPR 2810.1	Basic
	Number	Rev.
	Effective Date: October 27, 2004	
	Expiration Date: August 3, 2009	
Responsible Office: Center Operations Directorate		Page 37 of 41
SUBJECT: SSC Public Key Infrastructure (PKI) Procedural Requirements		

Attachment C: PKI Certificate Issuance and Account Information Memorandum

EXAMPLE ONLY

(Letters are subject to change depending upon varying requirements and circumstances of the actions required.)

FROM: NASA/IPSO, SDC Operations/PKI Registration Authority

SUBJECT: PKI Certificate Authorization

USERNAME:

CERTIFICATE REFERENCE NUMBER:

CERTIFICATE AUTHORIZATION NUMBER:

The NASA/IPSO SDC Operations/PKI Support, Stennis Space Center PKI Registration Authority, accommodates private and/or sensitive data subject to the Privacy Act of 1974 and the Computer Security Act of 1987. Your Certificate Authorization number is the key to this computing resource and should be safeguarded as you would other private or sensitive information.

The Username and Certificate Authorization number provided above permits you to gain initial access to the Entrust software. Use of this authorization number is prohibited prior to training. Once you have gained access, the system will prompt you to set a Profile Password. The new password must follow the Entrust Password Rules. It must have at least eight characters. It must contain one uppercase, one lowercase and contain at least one numeric character. It can contain any alphabetic or numeric characters, but must not contain many occurrences of the same character. The most occurrences of the same character allowed in your password are half of the length of your password. It must not be the same as your Entrust profile username. It must not contain a long substring of your profile username. The longest allowable profile username substring is equal to half of the length of your password. For example, the password "AlimcM*4" is valid because it meets the other criteria and contains only a three-character substring that is less than half the length of the password.

Select passwords with no direct connection to yourself. DO NOT use the following common password conventions:

- Any SSC reference or username, account or application information
- Your name (any combination), hometown, address, or telephone number
- Your birth date or social security number
- The names of your family members or loved ones
- The name of a pet

Stennis Procedural Requirements	SPR 2810.1	Basic
	Number	Rev.
	Effective Date: October 27, 2004	
	Expiration Date: August 3, 2009	
Responsible Office: Center Operations Directorate		Page 38 of 41
SUBJECT: SSC Public Key Infrastructure (PKI) Procedural Requirements		

- Your favorite automobile, boat, or sports franchise
- A name associated with your job (i.e., SHUTTLE, COLUMBIA)
- Any other item that bears a strong personal association.

Examples of preferred passwords:

H2OPlsNow! \$MonE!e! 2DayIs4U Car54whRU 340Hemi!

Always protect your password and your Entrust profile. An attacker must have your password and have access to your profile to masquerade as you. Never provide a copy of your profile to anyone else.

Software Installation:

Your PKI Entrust software is available for installation via online .exe file. To access and download your Entrust software:

1. *From your desktop open Network Neighborhood.*
2. *Open Entire Network.*
3. *Open Microsoft Windows Network.*
4. *Go to Sscoao and open*
5. *Then open Sscmimas.*
6. *Open the PROCEDURES folder*
7. *Open the Entrust icon (entrust.exe.) [\\Sscmimas\\PROCEDURES](#)*
8. *The Entrust install screen will appear (this may take a few moments)*
9. *Click the Next button to begin the installation and follow the onscreen commands to complete.*
10. *Read the Entrust Help/Tutorial first before proceeding further – this will give you the guidance you need for installing your Profile, which is essential to using the software.*
11. *Install your Profile – You will need the information provided in the beginning of this memo.*

Stennis Procedural Requirements	SPR 2810.1	Basic
	<i>Number</i>	<i>Rev.</i>
	Effective Date: October 27, 2004	
	Expiration Date: August 3, 2009	
		Page 39 of 41
Responsible Office: Center Operations Directorate		
SUBJECT: SSC Public Key Infrastructure (PKI) Procedural Requirements		

Attachment D: Acknowledgement of Receipt of Authorization and Account Information

EXAMPLE ONLY

(Letters are subject to change depending upon varying requirements and circumstances of the actions required.)

TO: SDC/PKI RA Operations
Building 1110
Stennis Space Center, MS 39529
Attn: PKI RA

FROM: _____

SUBJECT: Acknowledgment/Receipt of PKI Authorization and Account Information

I have received the above listed PKI Authorization and Account Information and acknowledge the following:

The information contained therein provides my personal Username and Authorization number that are for my use only. I will not divulge my number to anyone else.

I understand that I should not open the sealed envelope containing my Certificate or attempt to access the Entrust software if I have not completed required User training.

I will not write my password and leave it accessible to other persons. This includes highly visible areas such as my desk and on my terminal, or any other location that someone could gain knowledge of my password and username.

I will not use "weak" passwords that can be guessed easily, and will follow the guidance set forth in the attached procedure for creating "secure" passwords.

I will notify the PKI RA of any changes to the relevant information on my original request form. A change of mailing address, telephone number, department, change of leave status, change of status from contractor to government employee, government employee to contractor, and loss of requirement for access to PKI are all items that should be reported immediately.

I will read and understand the rules stated in the attached letter for access to PKI. If I do not understand the rules I will obtain clarification from the PKI RA. I also understand that non-adherence to these rules can cause the revocation of my certificate.

Signature _____ Date _____

Stennis Procedural Requirements	SPR 2810.1	Basic
	Number	Rev.
	Effective Date: October 27, 2004	
	Expiration Date: August 3, 2009	
Responsible Office: Center Operations Directorate		Page 40 of 41
SUBJECT: SSC Public Key Infrastructure (PKI) Procedural Requirements		

Attachment E: Notification of Revocation or Disabling/Suspension Action

<p style="text-align: center;">EXAMPLE ONLY</p> <p style="text-align: center;">(Letters are subject to change depending upon varying requirements and circumstances of the actions required.)</p>

TO:

FROM: NASA/IPSO, SDC Operations/PKI Registration Authority

SUBJECT: PKI Account Revocation and Suspension

The NASA/IPSO, SDC Operations/PKI Registration Authority, accommodates private and/or sensitive data subject to the Privacy Act of 1974 and the Computer Security Act of 1987. We have received a request for Revocation or Suspension/Disabling of User account _____.

Our records indicate the following reason for request for revocation or suspension/disabling:

- ☐ User Account no longer required
- ☐ User on extended leave
- ☐ User no longer part of Domain
- ☐ Dismissal or suspension for cause
- ☐ Compromise/suspected compromise of private key and/or User password and profile
- ☐ Change in Requester's/User's role (e.g., organizational change between Centers) or permissions
- ☐ Termination of employment
- ☐ Failure of Requester/User to meet specified obligations under the NPR and relevant policies
- ☐ Other: _____

The following actions have been initiated in response to this request. You will be notified of any other actions initiated by either the SSC IT Security Manager or the SSC RA.

- ☐ Account Revoked
- ☐ Account Suspended/Disabled
- ☐ Account Deleted

If your records disagree with the above provided information, please contact the PKI RA located in SDC Operations, Building 1110, Stennis Space Center at (228) 688-2116.

Date _____
PKI RA

Attachments: Receipt Acknowledgement

Stennis Procedural Requirements	SPR 2810.1	Basic
	<i>Number</i>	<i>Rev.</i>
	Effective Date: October 27, 2004	
	Expiration Date: August 3, 2009	
		Page 41 of 41
Responsible Office: Center Operations Directorate		
SUBJECT: SSC Public Key Infrastructure (PKI) Procedural Requirements		

Attachment F: Acknowledgement of Receipt of Revocation or Suspension/Disabling Notification

EXAMPLE ONLY

(Letters are subject to change depending upon varying requirements and circumstances of the

TO: IPSO/SDC Operations
Building 1110
Stennis Space Center, MS 39529
Attn: PKI RA

FROM:

SUBJECT: Acknowledgment/Receipt of Revocation and Suspension Notification -
For User Name_____

I have received notification regarding revocation or suspension/disabling of the above named PKI User account, and acknowledge the following:

I understand that key compromise, suspected compromise, or dismissal for cause is provocation for immediate revocation of User access and is considered a security incident.

I understand that reinstatement of revoked certificates is permitted only under certain circumstances.

I understand that in the case of an accidental key compromise that a Key Recovery Request must be completed in order to regain access.

I understand that misuse of PKI processes may constitute grounds for termination of privileges, administrative action, and/or civil or criminal prosecution.

Signature_____ Date_____